2009-05-01

Software Safety Strategy for US Navy Gun System Acquisition Programs

Rivera, Joey

Defense Acquisition in Transition

6TH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

Software Safety Strategy for US Navy Gun System Acquisition Programs

Joey Rivera, Paul Dailey

Software Engineering Ph.D. Students, Naval Postgraduate School

Background

- US Navy weapon and combat system acquisition programs are evolving
  - Drive to implement Open Architecture (OA)
  - Increasing levels of software complexity
- Acquisition and demonstration of safe software becomes a more challenging task
  - Increased safety risk, cost & schedule overruns
  - Difficulty proving system safety to independent review boards

Problem

- There is no standard methodology in place for program managers to follow regarding software safety
  - Current management practice varies from program to program
  - Reactive vs. proactive evaluation approach
  - Focus of this research: gun systems software safety

Software Safety Program Management Strategy Needed

- Methodical and effective approach
- Strategy goals
  - Reduce average number of safety issues
  - Improve process for handling issues encountered
  - Reduce surprises encountered during SSSTRP and WSESRB

Developing the Risk Management Strategy

- Identify common risks…
  - Among current gun system acquisition programs
  - For future OA software-based gun systems
- Develop mitigation strategies to address each common risk
- Combine into a program management level software safety risk management strategy

Identifying Common Safety Risks for Today's Gun Systems

- Conduct survey, discuss experiences & lessons learned
  - Program Managers & Safety Community Members
- Analyze SSSTRP process:
  - Panel members
  - Characteristics of systems being reviewed
- Research OA / COTS Specific Risks

Identifying Common Safety Risks for Today's Gun Systems (cont)

- Obtain SSSTRP reports on recent gun system acquisition programs
- Extract & catalog findings from each report
  - Categorize findings into project management and safety management areas
- Analyze data, identifying common risks & trends
  - Identify OA-related issues

Organize Findings from SSSTRP data

- Project Management
  - Project Planning
  - Requirements Management
  - Integration & Testing
  - Configuration Management
  - Validation & Verification
  - Risk Management
  - Deployment & Maintenance
- Safety Management
  - System Safety Program
  - Software Safety Program
  - Safety Risk Management
  - Safety Verification / Audits
  - Hazard Tracking
  - COTS, GOTS, NDI
  - Sim, Stim, Emulation

Category definitions are evolving via collaboration with various members of the DoD systems safety community

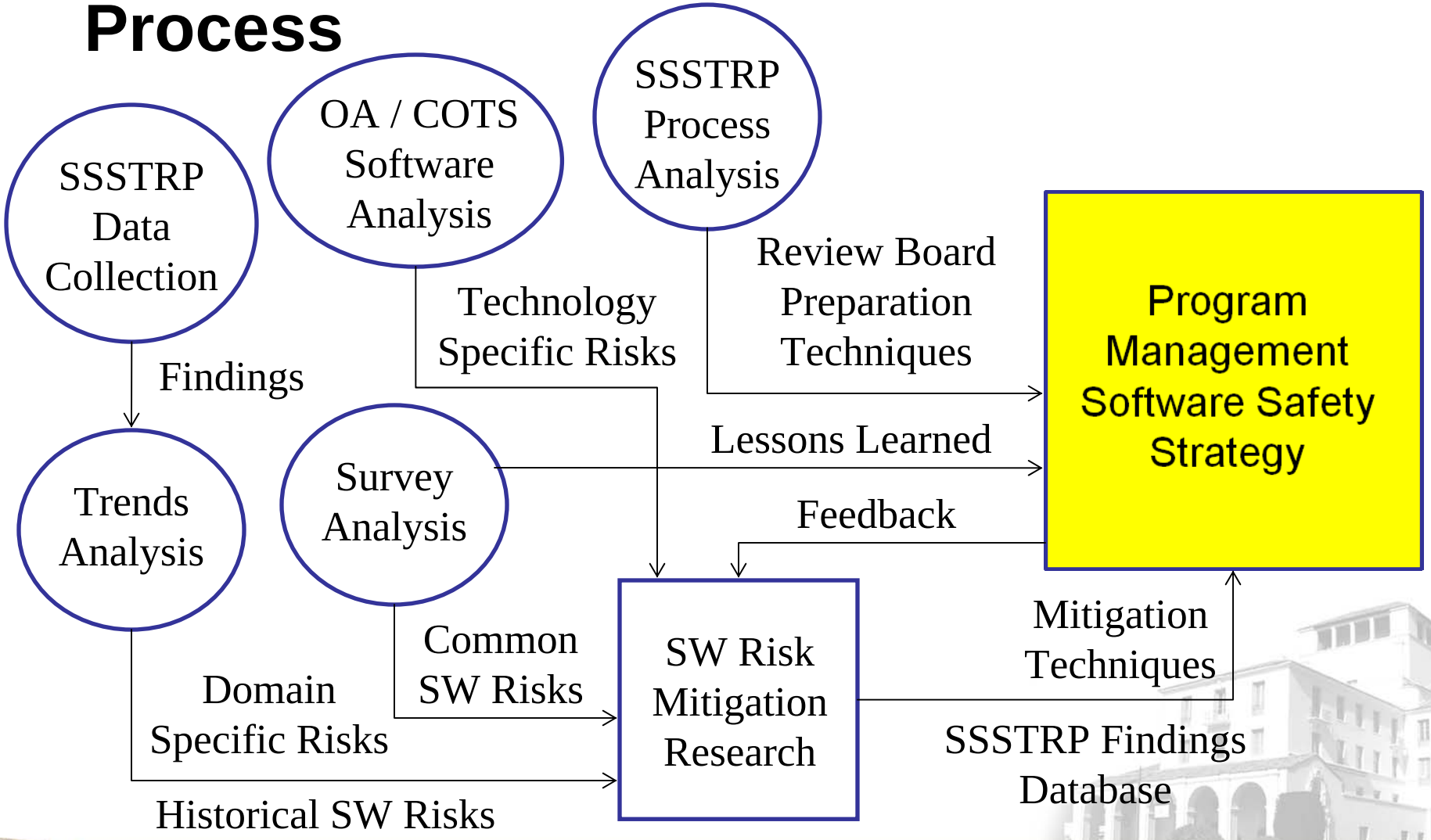
Developing Risk Mitigation Strategies

- Identify successful actions used to resolve historical issues
- Apply existing/proven risk mitigation methodologies from OA and PM domains
- Develop custom techniques if needed
- Continue a centralized SSSTRP findings database to track future opportunities

Developing Risk Mitigation Strategies (cont)

- Combine risk mitigation methodologies and techniques into a program management methodology
- Provide methodology and assessments of the content to program managers for review and use
- Acquire feedback if possible to improve methodology

Software Safety Strategy Development Process



Data Collection in Progress

Filename N3C5-G-10-146-1912.PDF
MK 34 MOD 4 - USS Bunker Hill (CG-52)
Purpose:

Concurrance to conduct structural test firings.

Finding Summary:

- Incorporate accurate data into software test build. (Insufficient Testing)
- Perform safety assessment after the modifications have been made.
- Verify and Validate software before structural testing
- Incorporate safety schedule into program schedule

- Perform interface safety assessment between training system and weapon.
- Show that all safety risks have been accepted in accordance to DoDI 500.2
- Establish a Hazard Tracking Database
- Provide status of prior SSSTRP Findings.

Comments:

The SSSTRP took exception to the fact that this program decided to seek concurrance to conduct structural test firings with software that was still under development. I suspect that the previous version of this software had been accepted by the SSSTRP but safety assessments need to be performed and presented to the SSSTRP. Also, the risks associated with the changes needs to be determined.

Example of data extracted from an SSSTRP report for current gun programs

Several years of historical SSSTRP data under analysis so far

Questions?